AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of IN THE MATTER OF THE SEARCH OF INFORMATION RELATED TO T-MOBILE TIMING ADVANCE LOCATION DATA WITHIN DEFINED SEARCH AREAS (See Attachment A).	4:24 MJ 2112 JSD **FILED UNDER SEAL** SIGNED AND SUBMITTED TO THE COURT FOR FILING FOR RELIABLE ELECTRONICS MEANS

APPLICATION FOR A SEARCH WARRANT

I, Rhonda Maratea, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that in the following property:

See Attachment A

This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A)

located in the _____ District of New Jersey, there is property

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

XX evidence of a crime

The search is related to a violation of:

Code Section		*Offense Description*
Title	Section	
18	2115	Burglary of Post Office
18	1708	Theft or receipt of stolen mail matter generally
18	371	Conspiracy

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

✓ Continued on the attached sheet.

❑ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the following is true and correct.

Rhonda Maratea
Applicant's signature

Rhonda Maratea, Inspector U.S. Postal Inspection Service
Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: March 8, 2024

Judge's signature

City and State: St. Louis, Missouri

Honorable Joseph S. Dueker, U.S. Magistrate Judge
Printed name and title

AUSA: Torrie J. Schneider

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION RELATED TO T-MOBILE TIMING ADVANCE LOCATION DATA WITHIN DEFINED SEARCH AREAS (See Attachment A).	No. 4:24 MJ 2112 JSD **Filed Under Seal** Signed and submitted to the court for filing by reliable electronic means

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Inspector Rhonda Maratea**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for records and information associated with certain cellular towers ("cell towers") and records generated by the cellular network that are in the possession, custody, and/or control of **T-Mobile**, a cellular service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile to disclose to the government copies of the information further described in Attachment B.

2. I am a Postal Inspector with the United States Postal Inspection Service ("USPIS") assigned to the St. Louis, Missouri Domicile office and have been since June 2016. During that time, I have worked on many investigations involving postal carrier robberies; facility burglaries; thefts of mail and arrow keys; and various fraud

schemes, including mail, wire, and bank fraud, as well as aggravated identity theft. Before becoming a Postal Inspector, I was a patrol officer for the City of Blue Island, Illinois for approximately five (5) years. I have received training on criminal investigative techniques and practices including robberies, burglaries, mail theft, and financial crimes. I have also conducted investigations, including the execution of search warrants, involving computers, cell phones, email addresses, and other electronic storage devices and their ability to commit and/or further the commission of crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that persons known and unknown, have committed violations of Title 18, United States Code, Section 2115 (burglary of a United States Post Office); Title 18, United States Code, Section 1708 (theft or receipt of stolen mail matter generally); and Title 18, United States Code, Section 371 (conspiracy). There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§

2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO WIRELESS PROVIDERS

6. In my training and experience, I have learned that the Provider is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

7. Based on my training and experience, I know that wireless providers can collect cell-site data about the subject phone. I also know that wireless providers such as typically collect and retain cell-site data pertaining to cellular phones to

which they provide service in their normal course of business to use this information for various business-related purposes.

8. In my training and experience, I have learned that T-Mobile is a company that provides cellular communications service to the general public. To provide this service, many cellular service providers maintain antenna towers ("cell towers") that serve and provide cellular service to specific geographic areas. Each cell tower receives signals from wireless devices, such as cellular phones, in its general vicinity. By communicating with a cell tower, a wireless device can transmit and receive communications, such as phone calls, text messages, and other data. When sending or receiving communications, a cellular device does not always utilize the cell tower that is closest to it. Additionally, cellular service providers such as T-Mobile also capture historical location data that is generated and derived from a cellular device's interaction with the cellular network. This information may include but not be limited to a cellular device's estimate distance from a particular cell tower and T-Mobiles network derived location of the device in latitude and longitude.

9. Based on my training and experience, I know that cellular providers, such as T-Mobile routinely and in their regular course of business maintain historical cell-tower log information, including records identifying wireless communications that were transmitted through a particular cell tower. For each communication, these records may include the telephone call number and unique identifiers for the wireless device that sent or received the communication ("the locally served wireless device"); the source and destination telephone numbers associated with the communication

(including the number of the telephone that called or was called by the locally served wireless device); the date, time, and duration of the communication; the cell tower(s) that handled the communication as well as the "sectors" (i.e. the faces of the towers) that received a radio signal from the locally served wireless device; and the type of communication transmitted (such as phone call or text message).

10. Furthermore, cellular providers such as T-Mobile in their regular course of business maintain certain types of location data associated with a cellular device based on that cellular device's interaction with the cellular network. For these interactions with the cellular network these records may include unique identifiers for the wireless device that interacted with the network ("the locally served wireless device'); the date, time and duration of the interaction with the network; the cell tower and sector (i.e. face of the tower) that was involved; the estimated distance from the tower and sector that the cellular device was located; and the estimated latitude and longitude of the cellular device. The previously mentioned location information is often contained within Timing Advance data, also known as True Call, that is captured and controlled by T-Mobile.

11. Based on my training and experience, I know that wireless providers typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers typically collect and retain information

about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the subject phone's user or users and may assist in the identification of co-conspirators and/or victims.

12. Because the cellular device generally attempts to communicate with the closest unobstructed tower, by reviewing the above-described information, your affiant and other law enforcement officers can determine the approximate geographic area from which the communication originated or was received.

13. Based on my training and experience, I also know that each cellular device is identified by one or more unique identifiers. For example, with respect to a cellular phone, the phone will be assigned both a unique telephone number but also one or more other identifiers such as an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The types of identifiers assigned to a given cellular device are dependent on the device and the cellular network on which it operates. When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna

or tower to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

14. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service used, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number).

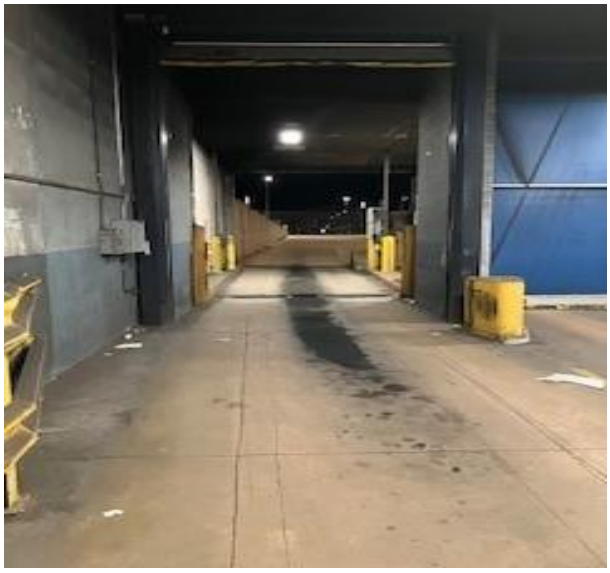
PROBABLE CAUSE

15. On February 14, 2024, USPIS learned of a burglary of the St. Louis Processing and Distribution Center ("P&DC"), 1720 Market St., St. Louis, Missouri 63155, resulting in the theft of four United States Postal Service (USPS) registry sacks, which contained 13 pieces of registered mail.

16. When sending registered mail, a customer must file USPS form 3806, Registered Mail Receipt, which requires the customer to declare the full value of the

mail piece. Using postal databases, this affiant learned that the total estimated monetary value of the stolen registry mail pieces is approximately $183,000.

17. On February 14, 2024, witness "M.M." stated that at approximately 4:25 a.m., they were operating a tractor/truck in the rear truck parking lot of the P&DC and attempted to enter the truck entrance door. At that time, M.M. observed a gray Jeep stop short of the entrance door, which blocked M.M. from driving entering. M.M. observed two black male subjects exit the P&DC near the truck loading docks. The subjects were carrying registry bags and entered the passenger side of the gray Jeep. M.M. described the registry bags as white bags with orange pieces of paper on them.



Inside view of truck entrance

Outside view of truck entrance and exit doors

Truck loading dock doors

18. M.M. described the suspects as two black males, wearing black hoodies with an unknown matching white logo on the front, surgical masks, and hoods. M.M. described the suspect vehicle as a 1999 to 2004 gray Jeep Grand Cherokee with tinted windows and no front license plate.

19. On February 14, 2024, another witness, "J.H.", stated that at approximately 4:00 a.m. they observed a 1990's Jeep with tinted windows parked on Clark Street across from the P&DC's rear truck parking lot. J.H. observed two

subjects walking across the rear truck parking lot toward the truck entrance and exit doors.

20. J.H. said the subjects entered the P&DC through the truck entrance and exit doors. J.H. stated that the subjects were "scoping around" and appeared to be communicating with each other. J.H. saw the subjects standing face-to-face while wearing surgical facemasks, so it appeared they were talking to one another. The subjects then left the P&DC empty-handed and entered the Jeep, still parked on Clark Street. One subject got into the front passenger seat, and the other got into the rear passenger seat.

21. Later that same day, J.H. observed the same two subjects, each holding registry bags, running from the P&DC. J.H. heard someone yell "come on man," but did not see a vehicle this time.

22. J.H. described the first suspect as a short, black male with dreadlocks, wearing a surgical facemask, a black hoodie with a white Nike swoosh in the corner of the chest, and navy jogging pants. J.H. described the second suspect as a tall, black male with short hair, wearing a surgical facemask, a black hoodie with white Nike swoosh in the corner of the chest, jeans, and talking on a cell phone.

23. Inspectors requested the assistance of the St. Louis Metropolitan Police Department's Real Time Crime Center ("RTCC") to search license plate reader data and traffic cameras for vehicles matching the description(s) given by witnesses. RTCC found a silver SUV in the area of P&DC, at or near the time of the burglary, specifically on 18th and Clark Streets at approximately 4:25 a.m.

24. Before the burglary, the first street camera to capture the silver SUV was near the intersection of Lafayette Avenue and Tucker Boulevard at 3:55 a.m. It was then captured turning northbound onto Truman Parkway from Lafayette Avenue. As it traveled north on Truman Parkway, it passed, in short succession, Park Avenue; Chouteau Avenue (Truman Parkway turns into 18th Street at this point); Papin Street; and Clark Street.

25. RTCC also provided the silver SUV's direction of travel after the burglary, which included many of the same intersections. Specifically, at 4:25 a.m., the SUV turned southbound onto 18th Street from Clark Street and, again, in short succession crossed Papin Street and Park Avenue before turning eastbound onto Lafayette Avenue. The silver SUV then turned southbound onto 13th Street and finally onto Tucker Boulevard from Soulard Street traveling in the direction toward Interstate 55. According to RTCC, the silver SUV is not seen on street cameras again after that time.

26. On February 29, 2024, Inspectors received information from a local law enforcement officer that a confidential source (CS) had information about the burglary. According to the CS, Roland Campbell ("Campbell") is a person of interest. Through open-source research, investigators identified phone number (314) 771-9368 and 1343 Delvin Street, St. Louis, Missouri 63110 as being associated with Campbell.

27. A search of the cellular towers servicing the area of the burglary and the direction(s) of travel of the silver SUV, a likely suspect vehicle, at the time of the burglary, as well as immediately preceding and following it, may help identify those involved. In addition to the P&DC at 1720 Market Street, St. Louis, Missouri 63155, Inspectors identified Soulard Street at Tucker Boulevard, as the last known location the silver SUV was seen on video surveillance.

28. Based on my training and experience, individuals carry their cellular phones on their person or in a very close vicinity whether it is day or night. Further, most individuals have their own cellular phones, so it is likely the cellular phone the

subject is using and/or that registers with the cellular tower providing service in the general geographic area of the crime belongs to them.

29. Based on my training and experience and the above facts, information obtained from cellular service providers, such as T-Mobile, reveal cell towers and, where applicable, the sectors that were used and the estimated location information (the estimated distance from the tower and sector and estimated latitude and longitude) of a given cellular device engaged in a particular communication or interaction with the cellular network. This information can be used to show that the device was in the general vicinity of the cell tower or an estimated location at the time the communication or network interaction occurred. Thus, the records described in Attachment A will identify cellular devices that were in the vicinity of:

a. 1720 Market Street, St. Louis, Missouri 63155 on February 14, 2024 between 3:50 a.m. and 4:35 a.m. (CST)

b. Soulard Street at Tucker Boulevard, St. Louis, Missouri 63104 on February 14, 2024 between 3:50 a.m. and 4:35 a.m. (CST)

AUTHORIZATION REQUEST

30. Probable cause exists to believe that the records requested contain evidence related to identifying Campbell, and other persons unknown, who committed violations of Title 18, United States Code, Section 2115 (burglary of a United States Post Office); Title 18, United States Code, Section 1708 (theft or receipt of stolen mail matter generally); and Title 18, United States Code, Section 371 (conspiracy). Based on the foregoing, I request that the Court issue the proposed

search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

31. I further request that the Court direct T-Mobile to disclose to the government any information described in Attachment B that is within its possession, custody, or control. Because the warrant will be served on T-Mobile, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

I state under the penalty of perjury the foregoing is true and correct.

Rhonda Maratea

Rhonda Maratea
Inspector, U.S. Postal Inspection Service

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on March 8th, 2024.

JOSEPH S. DUEKER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
4:24 MJ 2112 JSD
Property to Be Searched

This warrant applies to a Timing Advance "True Call" area search for all records and unique device/user identifiers pertaining to Timing Advance location information during the following listed dates, times, and distance from the GPS points:

1. Location #1

   1720 Market Street, St. Louis, Missouri 63155

   GPS coordinates: 38.627135034586935, -90.20486953824681

   Distance from Location: .25 Miles

   Date: February 14, 2024 Time: 3:50 a.m.- 4:35 a.m.

2. Location #2

   Tucker Boulevard at Soulard Street, St. Louis, Missouri 63104

   GPS Coordinates: 38.612075089903925, -90.20694611502124

   Distance from Location: .25 Miles

   Date: February 14, 2024 Time: 3:50 a.m. – 4:35 a.m. (CST)

ATTACHMENT B
4:23 MJ 2112 JSD

Items and Information to be Seized and Searched

All information that constitutes evidence of violations of Title 18, United States Code, Section 2115 (burglary of a United States Post Office); Title 18, United States Code, Section 1708 (theft or receipt of stolen mail matter generally); and Title 18, United States Code, Section 371 (conspiracy), on February 14, 2024, involving Roland Campbell and other unknown persons, including location information and identifying information as specified below.

1. T-Mobile shall provide responsive data for each search area described in Attachment A and are required to disclose to the United States all records and other information (not including the contents of communications) about all communications made and all cellular device interactions with the network that have generated location information that falls within the defined search area during the corresponding timeframe(s) listed in Attachment A, including records that identify:

a. the unique identifiers for each wireless device that generated a Timing Advance "True Call" record within the search area for each location, including International Mobile Subscriber Identifiers ("IMSI"), International Mobile Equipment Identities ("IMEI"), and the make and model of the device;

b. the starting and ending date/time of the connection along with the duration;

c. for each communication with the network the tower and the "sector(s)" (i.e., the face(s) of the tower(s)) that received a radio signal from the locally served wireless device for both starting and ending points of the communication;

d. the service type for the communication and;

e. the estimated latitude and longitude (along with confidence level) and the distance from the tower for both the starting and ending points of the communication contained within the Timing Advance "True Call" records.

2. These records should include records about communications and cellular device interactions with the network that were initiated before or terminated after the timeframe(s) identified in Attachment A if some part of the communication occurred during the relevant timeframe(s) listed in Attachment A.

3. It is anticipated that identifying information will be requested for devices whose characteristics meet any of the following criteria:

a. Devices whose cellular network records place them in at least two of the locations and/or

b. Devices whose cellular network records, including distance from the tower and/or network derived latitude and longitude, are consistent with the facts of the investigation and would not solely reflect a device passing through.

4. It is noted, however, that no subscriber information (including, but not limited to, name or phone number associated with the identifiers) or location information outside the initial search criteria is authorized by this warrant and additional legal process will be submitted.

5. To the extent that any device information other than devices relevant to this investigation is collected by law enforcement, law enforcement will not make investigative use of it absent further order of the court, other than distinguishing the devices relevant to this investigation from all other cellular devices.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS UNDER FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by T-Mobile, and my title is _____. I am qualified to authenticate the attached records because I am familiar with how the records were created, managed, stored, and retrieved. I state that the attached records are true duplicates of the original records in the custody of T-Mobile. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of T-Mobile, and they were made by T-Mobile as a regular practice; and

b. such records were generated by T-Mobile's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of T-Mobile in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by T-Mobile, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature